MFA is A Necessary Chore!
Exploring User Mental Models of Multi-Factor Authentication Technologies

Sanchari Das
Indiana University
Bloomington
sancdas@indiana.edu

Bingxing Wang
Indiana University
Bloomington
bw10@indiana.edu

Andrew Kim
Indiana University
Bloomington
anykim@indiana.edu

L. Jean Camp
Indiana University
Bloomington
ljcamp@indiana.edu

Abstract

With technological advancements, traditional single-factor authentication methods, such as passwords, have become more vulnerable to cyber-threats. One potential solution, multi-factor authentication (MFA), enhances security with additional steps of verification. Yet, MFA has a slow adoption rate among users, and frequent data breaches continue to impact online and real-world services. Little research has investigated users' understanding and usage of MFA while specifically focusing on the their mental models and social behaviors in a work setting. We conducted semi-structured interviews with 28 individuals (11 experts, 17 non-experts), while focusing on their risk perceptions, MFA usage, and understanding of required technologies. We identified that experts treated MFA as a useful added layer of authentication, while non-experts did not perceive any additional benefits of using MFA. Both non-experts and experts expressed frustration with MFA usage, often referring to it as a 'chore.' Based on these findings, we make several actionable recommendations for improving the adoption, acceptability, and usability of MFA tools.

1. Introduction

The increased usage of online applications has been challenging for cybersecurity. Identity theft and phishing are rising concerns [1], with 76% of global organizations reporting phishing attacks in 2018 alone [2]. As a solution, authentication and authorization has been the major backbone of access control for online applications and services [3]. It provides identity verification of a user through trusted device(s), granting resource access to the verified entity [4]. Traditional single-factor authentication (SFA) methods, like passwords, have served as the primary authentication strategy for a long time [5]. However, under the increasing complexity of threats on the Internet, passwords [6] are susceptible to several security vulnerabilities [7]. Thus, we cannot rely on SFA for mission-critical sectors, such as finance, health care, or government [8]. In addition to traditional passwords, multiple factors of authentication are proposed as a solution to mitigate such issues, including federated sign-on, graphical passwords, biometrics, hardware tokens, visual tokens, and others [9, 10].

Multi-factor authentication (MFA) has been proposed to address vulnerabilities in SFA systems [11] by adding multiple layers of authentication[12]. In addition to asking for the passphrase, called "what you know," MFA enhances security by requiring the presence of other factors for successful user identity verification, like "what you are" and "what you have" [13]. Common secondary methods include personal identity verification devices (smart cards, USB tokens) [14, 15], time-based one-time password tokens (HMAC-based token applications, hardware tokens) [16], and the combination of bio-metric (fingerprints, face) [17] and hardware security devices (TPM, Secure Enclave) [18]. Popular examples of this system include mandatory verification codes for online banking [19] and FIDO U2F authentication tokens [20]. Despite its benefits, usability and acceptability of MFA tools still remains a challenge, based on users' risk perceptions [21, 22]. Das et al.'s work was focused on understanding users' experience with 2FA adoption. While we were motivated by their work, we focus on understanding users' mental models and risk perceptions regarding online data security.

To help us understand users' perceptions of MFA technology, we conducted semi-structured interviews, where we asked users about their daily interaction with passwords, 2FA, and MFA tools and devised a sketching exercise followed by questions regarding their risk perception. We specifically addressed the following research questions:

- *RQ1. What are user's risk perceptions of online threats?*
- *RQ2. How does computer and security expertise level affect adoption of MFA tools?*
- *RQ3. What are the common perceptions and understandings of how authentication methods, such as passwords, 2FA, and MFA work?*
- *RQ4. How are authentication methods applied in work and personal settings by users?*

Our study shows how users' expertise levels can impact the adoptability (and thus, effectiveness) of security tools. Our research not only reveals detailed encounters with MFA through the interviews, but also further explores users' risk perception. We provide critical details about applications of MFA tools in work and educational settings. We detail background literature exploring authentication technologies and risk mental models in section 2. Section 3 provides a detailed description of the study protocol, followed by the critical findings of the study in section 4. We conclude with the major factors that prevent MFA's wide adoption, while discussing our findings in section 5 and recommendations in section 6.

URI: https://hdl.handle.net/10125/64411
978-0-9981331-3-3

2. Related Work

While multi-factor authentication dramatically improves online data security, a slow rate of MFA adoption has been observed due to negative user perception of MFA technologies [23]. Security and usability are both essential for ensuring secure access control [24]. Current security and privacy tools, such as Tor [25], Pretty Good Privacy (PGP) [26], and MFA [27] have been found to have certain negative impacts on the user experience, which prevents them from being widely and correctly utilized. For instance, in the case of PGP, users experienced usability issues due to the complexity of Public Key Infrastructure (PKI) [28, 29]. While implementing new tools to enhance security, researchers and practitioners often forget about the users' expertise in the domain, which leads to knowledge and usage problems [26].

2.1. Multi-Factor Authentication

Traditional MFA involves two or more methods for identity verification beyond the factor of "what you know". Popular methods utilize strong, definitive, and real-time, triangulated verification [30] to ensure users' identity and achieve security. Current common methods have their own advantages and limitations, depending on the application and users' expertise. Nag et al. proposed a new MFA system that eliminates the traditional static procedure of enrollment. Instead, factors such as devices' fingerprints, users' behavior, and geo-location data are continuously collected in a dynamic, adaptive, and continuous multi-factor authentication scheme [31]. In the context of authentication, such factors are verified together with a passphrase. It achieved additional security while lessening the burden for users to use the same set of authentication processes in less trustworthy environments.

Huang et al. applied a distributed and decentralized robust MFA system at a large scale [32]. Existing multi-factor technologies primarily rely on a centralized set of servers, which adds the risk of a single point of failure. A distributed design helps to improve the availability of service and adds to users' confidence [33]. Bhargav et al. pointed out that the risk of identity theft increases with the adoption of biometric authentication systems [34]. In the context of privacy, Jiang et. al examined and enhanced the practice of hashing biometrics to removes personally identifiable information (PII) [35].

Paepcke et al. interviewed information workers in multiple technical areas to understand the needs of users in technical work settings and provided design recommendation for improved information search and retrieval [36]. Their work provided tools for designing usable computer and information management systems. These technological advancements in MFA and security enhancing tools in general, improve security to a great extent; however, the same cannot be said for the users' acceptance of these tools. Thus, through our research, we sought to understand the user perspective.

2.2. User Expertise and Security Awareness

Rajivan et al. provided evidence of a correlation between users' knowledge level and users' security behavior by studying 898 participants and their security practices [37]. Gallagher et al. also showed that expertise level is a strong determinant of usage patterns in Tor [38]. Stanton et al. discussed the correlation between users' technological expertise and their security awareness [39]. These previous works found users' security expertise was aligned with their risk perception and attempts to protect their data, and they characterized security behaviors from "basic hygiene" to "intentional destruction."

Albayram et al. studied the difference between the 2FA/MFA adoption rate among users after watching introductory videos of MFA based on three themes (risk, self-efficacy, and contingency) [40]. They identified a higher adoption rate after viewing the videos on self-efficacy and risk. They suggested improvements on user education of risk awareness and development of self-efficacy. Despite the impact of security expertise on actual practices, studies on two-factor or multi-factor authentication have seldom explored the impact of expertise level, with a few exceptions [21, 15, 10]. We integrated the expertise knowledge with the usage and perception of MFA to understand the correlation between these two key elements that enhance security hygiene. We also integrated survey-based factor analysis along with interviews to ensure we have more accurate data from our participants. Additionally, to explore users' risk mental models, we adopted the sketching method by Gallagher et al. [38].

2.3. User Experience of MFA

Braz et al. pointed out that human factors and graphical user interface (GUI) design impact users' overall experience with multi-factor authentication [24]. Das et al. studied users' experiences with FIDO U2Fs and revealed that issues with enrollment and verification have caused troubles for users choosing to use the hardware token [21]. Weir et al. conducted experiments in the scenario of phone-based banking and suggested that such additional verification slowed down the banking process [41]. Reynolds et al. studied the YubiKey, where they focused on cases of MFA usability in desktop and web applications and identified major user failures in a majority of U2F applications, especially during the on-boarding (setup) procedures [42]. Colnago et al. studied the user experience of MFA in the context of organization-wide deployment, such as universities [43]. They collected data from the university's IT office for detailed statistics on MFA usage. They suggested improvements in implementation design and strategic messaging for better user adoption.

In our research, we explore the usability and acceptability of MFA technologies by analyzing users' attitudes towards new technology, while exploring users' technological awareness. Our study on mental models based on previous studies [44, 45] will help the research community in understanding users' pain points with MFA usage while guiding technology experts through design and architectural recommendations.

3. Methods

To answer the RQs mentioned in section 1, we performed a series of organized studies regarding users' expertise and MFA experience. These methodological approaches include an extension of Gallagher et al.'s studies on Tor [38], a semi-structured interview, and a qualitative analysis of user reviews of MFA applications and services. Figure 1 shows a snapshot of our study design and participant workflow.

3.1. Recruitment and Data Collection

We recruited participants for survey and real-world studies through flyers, mailing lists, social media, and advertisements across other platforms. We conducted pre-screening surveys to learn about their technological interactions. We then conducted semi-structured interviews with a selected set of participants and implemented a sketching exercise to evaluate their risk perceptions, specifically focusing on online data authentication and authorization. The subsections below describe the details of our recruitment procedure and study design. The protocol and the study was approved by the organization's ethical review board.

3.2. Pre-Screening Survey

For recruitment, our aim was to find users who come from diverse backgrounds with a common interest in MFA tools. We evaluated their expertise based on pre-defined and researched survey questions implemented in research studies by Das et al. [21] and Rajivan et al. [37]. Many of the participants expressed frustration and distress when they had to use MFA/2FA as a mandatory authentication for any of their personal or professional activities. One hundred twenty-seven participants answered our pre-screening survey. We particularly selected those participants who use MFA in their daily life in some capacity in order to understand the usability issues faced across different platforms.

3.3. Participants

Based on our pre-screening survey, we set up semi-structured interviews focusing on the MFA day-to-day usage of individuals who expressed interest in participating in the study. Overall, we interviewed 28 individuals, who were asked to perform a sketching exercise. We also had a brief survey at the end of the interview where participants were asked a few MFA-related questions. Apart from ensuring that each participant was above the age of 18, we did not collect personally identifiable information to respect the privacy concerns of the participants.

3.4. Study Protocol

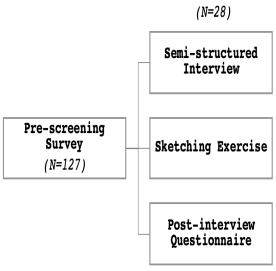

Figure 1. Flow Chart of the Study Protocol

As introduced by Kearney and Kaplan [46] and implemented in the Tor study by Gallagher et al. [38], we also developed a sketching exercise after the interview for the participants to explain what they think about authentication technologies. We first asked them to draw about the most common SFA technique, which is passwords. Next, we asked them to draw what they thought about 2FA, and finally, they drew about MFA. Many participants felt hesitant to express their thoughts through their drawings, since they felt that they would be evaluated based on their artistic abilities. Thus, we addressed their concerns and transcribed how they felt while sketching in order to avoid any artistic influence on their understanding of the concepts of authentication.

After the interview and the sketching exercise, we asked the participants to fill out a post-interview questionnaire, where they answered questions about their MFA usage and tools they use to implement multi-factor authentication, ranging from simple messaging-based one-time passwords to biometric authentication. In the post-survey, we also asked computer and security expertise questions to answer our research questions. Our standardized factor analysis is based on previous work by Rajivan et al. [37]. As shown in Figure 2, those who scored more in the qualified conditions in either computer questions or security questions (adjusted with final precision factors) were termed as 'Experts,' while those who did not meet at least one category of the standard were termed as 'Non-Experts.' We also asked questions about the nine dimensions of risks to analyze the threat models of the users. The nine dimensions of risk perception are: Voluntary, Immediacy, Control, Science, Expertise, Catastrophic, Chronic, Severe, and Newness [47], as detailed in section 4.1.

Transcription and Coding: Before starting the semi-structured interview, we provided the participants with details regarding how their data will be stored or accessed. As mentioned, we did not store any personally identifiable information about the participants and used pseudonyms for analysis purposes. We then took consent from the participants to record (audio) the conversations. Two researchers transcribed the audio recordings of the interview, which were verified by a third researcher to avoid any data loss or misinterpretation. The interviews ranged from anywhere from 20 minutes to an hour. Though difficult and time consuming, the researchers did not use any tools apart from the audio recording device at low speed to transcribe the data due to privacy concerns. Once the transcription was done and verified by another researcher, we started the qualitative coding procedure.

All the interviews were taken in-person, and we specifically avoided any telephone or virtual conversations, since our study protocol required a sketching exercise. All the interviews were conducted by the primary researcher of the paper. Most of the questions asked were open-ended questions to allow the participants to express what they felt about their daily MFA and 2FA interactions. We are using 2FA and MFA interchangeably here, since many participants considered their work server or their work computers as another mode of authentication. To delve deeper, we specifically asked users to compare and contrast between 2FA and MFA. Though a small fraction of participants understood the difference, most of them considered 2FA as the only MFA they know about. If asked further, some expressed other factors, which we have described in detail in section 4.

The qualitative coding consisted of three steps- open, axial, and selective coding [48]. Two researchers, who were trained in qualitative coding, coded a subset of the transcribed data and generated a list of 136 codes.

Later, these open codes were grouped to create axial codes, and we performed selective coding to specifically answer questions about mental models, threat models, expertise influence, frequency of usage, willingness to use, and others. The researchers met two times each for the different stages of coding; for open coding, codes from both the researchers were considered to maintain an open subset. Both the researchers then met to group them into axial coding. For the selective coding, the two researchers coded the set separately and found an inter-rater reliability rate of 76.8%. This followed a round of open discussions, based on which another round of coding was conducted, where the inter-rater reliability rate was noted as 89.5%. Based on the second round of discussions of the selective coding, the data was analyzed.

Factor analysis: For all questions in the survey related to computer and security expertise, weight-based scores were given to each component. Some of the options were presented as a binary choice (i.e. yes or no), while others were presented as a 5-point Likert scale, from strongly disagree to strongly agree. We assigned values from -2 to 2 for degree-based questions. All the questions were based on the model of Ravijan et al. [37]'s work, and we performed factor analysis using the validated weight model. The weight assignment chart is presented in Figure 2. Certain components have negative contributions to factorized scores. We define "Computer Experts" as people who have computer expertise scores over 3 out of 5 in our questionnaire and "Security Experts" as people who have security expertise score over 2.4 out of 4. More details have been provided in section 4.

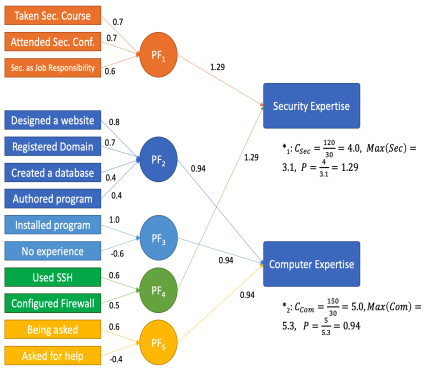

Figure 2. Weight Assignment for the Factor Analysis with Explanation of Precision Scores

These categories provided an important baseline standard for our findings, as explained in section 4, where we performed clustered and factorized analysis on specified metrics.

4. Findings

Our findings uncovered that users were aware of online security threats, but they occasionally failed to take proper mitigation procedures, including utilizing security tools. While experts demonstrated a systematic understanding and usage of multi-factor authentication, non-experts showed a lack of knowledge about MFA, a failure to distinguish between 2FA and MFA, and limited usage of MFA. Furthermore, both groups of users identified issues and concerns with current MFA technology.

4.1. Risk Perception

We evaluated risk perceptions across users through nine parameters: Voluntary, Immediacy, Control, Science, Expertise, Catastrophic, Chronic, Severe, and Newness. Table 1 describes users' knowledge of security threats such as phishing. We primarily focused on explaining the online risk in terms of phishing, since a majority of users (72.8%) expressed a good understanding of phishing as a common cybersecurity attack. While the data showed that users were aware of online threats, a significant portion of users expressed an inability to mitigate security threats using proper resources.

Perceptions	Agree	Disagree
Voluntary	14	14
Immediacy	22	6
Control	10	18
Science	17	11
Expertise	12	16
Catastrophic	26	2
Chronic	23	5
Severe	27	1
Newness	22	6

Table 1. Evaluation Factors of Risk Perception

The nine risk perception (Agree-Disagree) based questions were:

1. Voluntary - I can control the risk of my online account being taken over or being phished.
2. Immediacy - The harm of being locked out of my account would be immediate.
3. Control - If I am exposed to online risk, I can mitigate the harm.
4. Science - Experts understand phishing and know how to protect me from it.
5. Expertise - I understand phishing and know how to protect myself.
6. Catastrophic - Phishing is widespread and affects many people, and not only for targeted individuals.
7. Chronic - Phishing is everywhere, it's a constant exposure.
8. Severe - The effects of phishing are very severe.
9. Newness - Phishing is a new kind of risk.

4.2. User Expertise

Unsurprisingly, we found significant differences between expert and non-expert user perceptions of MFA tools and general security awareness. Experts demonstrated a high level of understanding of multi-factor authentication, while non-experts misinterpreted and oversimplified it. Notably, not all

technologically-aware users exhibited a higher level of security expertise, indicating that technological knowledge might not always correlate with security expertise. Based on the methodology adopted and factor analysis performed by Ravijan et al. [37], we adjusted the weight distribution by calculating the precision score for the expertise evaluation. The precision score was developed by conducting the expertise evaluation among 30 randomly sampled participants different from the sampled participants for our experiment. We found that the mean scores for security expertise was 120 and that of computer expertise was 150. Based on these scores, the precision scores were calculated as 0.94 for computer expertise and 1.29 for security expertise. Without any precision score adjustment, the maximum score a participant can gain for security expertise was 3.1 and 5.3 for computer expertise.

Any participant was termed as an expert if they had more than 60% on these scores. For a participant to be a security expert, they needed to score more than 2.8 and for computer expert, they needed to score more than 3.5. Figure 2 mentions the process of expertise calculation. We define expert as participants that were qualified as expert in at least one of the expert groups, and by that definition, we have 11 users as experts and 17 as non-experts in total.

4.3. Mental Models

During the interview, we attempted to discover the participants' understandings of MFA through semi-structured interviews (developed based on previous studies, such as those by Camp [49] and Liu et al. [50]) and sketching exercises. While both groups of participants (experts and non-experts) expressed frustration with MFA usage, the experts showed a better understanding of how MFA works than the non-experts.

Experts Treat MFA as Additional Verification: The experts understood the concept of authentication, as well as MFA. When describing how authentication works, the experts focused on the verification combined with certain factors. For example, one participant demonstrated the authentication flow in a sketch. In Figure 3, the expert explained the particular factor of passwords, as well as other factors' usage in the authentication process, such as a door to the house. It was interesting to find how users indicated their personal space and physical safety with authentication technology and online data protection. We kept the interpretation and representation open-ended for those who were not entirely comfortable drawing; thus, participants also wrote a few words alongside the sketches. In another interview, one expert user pointed out that additional factors provide additional verification: *"It is another kind of verification"* (P1, Expert)

Typically, the experts viewed MFA from the perspective of having multiple protective layers. Moreover, most of them were able to identify duplicated factors in multi-factor authentication. For instance, one expert stressed that all points of security should be distinct from each other in order to avoid device dependencies. In the interview, another expert compared two-factor authentication and multi-factor authentication as shown in Figure 4. Keys are an important component of protection in the real world, and many users represented MFA using the same analogy.

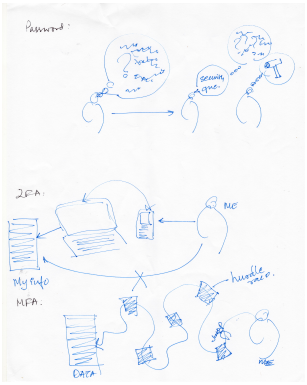

Figure 3. An Expert's Understanding of the Multi-Factor Authentication Flow and Other Factors

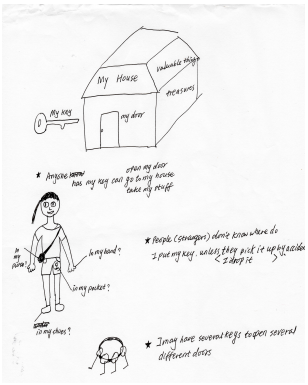

Figure 4. An Expert's Sketch of a 2FA/MFA Comparison

Non-Experts View MFA as a Security Service: Most non-expert users treated MFA as "added security." They did not care about the internal implementation of the authentication system or other factors, but instead focused on the result. For instance, one non-expert participant described MFA as "another protection." But none of them were clear about what MFA protected them from. They perceived MFA as a necessary 'chore,' and they often indicated that they would opt out of it given the choice: *"It is kind of double protection, but I guess my password is secure enough and this is unnecessary."* (P2, Non-expert)

"...it is frustrating to use MFA, specifically while I am working on something important. I do not think I need so much protection for my data." (P3, Non-expert)

Non-experts also found MFA to be useless and thought that additional layers of security increased their workload to a point where they found little to no benefits. For instance, a non-expert user felt that 2FA added trouble to daily authentication and that MFA added even more.

Unlike the experts, few non-expert users were able to identify the different modes of MFA (e.g. FaceId, TouchId, passcodes, etc.) However, they realized that multi-factor authentication provided more security for online applications. Most of the non-expert users presented MFA using methods-based approaches in the sketching exercise. For instance, non-expert P11 drew

SPF protection as well as a sun umbrella to explain the effects of MFA. Figure 5 shows that they knew what 2FA/MFA is in theory, as they linked it with a real life example of protecting themselves under the sun. However, when asked what they are protecting through MFA, they were unsure: *"I guess, it will protect my account. I don't know how it will do it. It is unnecessary. Sometimes, you might not want to have any sunscreen lotion to protect yourself from the sun. How about you want a tan?"* (P11, Non-expert)

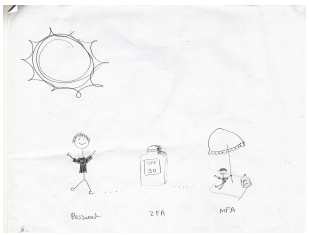

Figure 5. One Non-Expert Uses a Metaphor to Explain How Multi-Factor Authentication Works

Non-experts failed to distinguish MFA from 2FA. Many non-experts did not understand what MFA is at all; for 2FA, they could relate one-time passwords, voice authentication, or even push notifications. However, they seldom thought that more than two-factors were necessary. One participant explained: *Passwords are enough! 2FA is in itself a hassle, let alone be other factors. How can they hack my phone and my password, they cannot!* (P7, non-expert)

Apart from noting the non-expert treatment of multi-factor authentication as a service, we also identified that a few non-expert users treated the first MFA service vendor they used as a representation of all MFA tools. For instance, in interviews where we asked users about their understanding of two-factor authentication and MFA, their answers referred to a particular service vendor: *"Is that a Duo?"* (P2, Non-expert)

4.4. Discovery and Use of MFA

We examined how the participants started to utilize multi-factor authentication and their motivations for doing so. Both experts and non-experts showed a willingness to protect their high-value accounts using MFA technology, but the non-experts reported issues in successfully finding the MFA enrollment system. We asked participants about their intentions to protect accounts using MFA technologies and about other approaches they planned to use for protecting accounts. Among expert users, four out of 11 (36.7%) indicated they would protect all accounts using MFA, and the others indicated that they protect work-related assets using MFA. Among the non-expert users, six out of 17 (35.3%) indicated that they would protect all accounts, two did not prefer to protect any accounts using MFA, and the others preferred to just protect work assets.

Experts' Password Behavior and MFA Preferences: Among expert users, most participants exercised the recommended safety procedures for creating and managing passwords, using unique passwords for each website to mitigate the risk of password breaches. Four participants also reported the usage of password managers for password generation and storage, and three explained their awareness of memorization issues for long passphrases (which is one motivation for using technological methods for password management). One user explained their intention to replace traditional passwords with biometrics. Expert users expressed a consistently strong preference for modern technologies, such as security keys and mobile notifications, for multi-factor authentication. However, one expert was also not satisfied with the extra time cost in launching MFA applications. Two of them also preferred biometrics for multi-factor authentication. In addition, six expert users expressed concerns about the actual security provided by security questions.

Non-Experts' Password Behavior and MFA Preferences: Non-expert users showed a generally positive trend in their password management behavior. However, four of them did not utilize long or complex passphrases, due to the inconvenience of memorizing them. Ten non-experts expressed an interest in trying security keys. For multi-factor authentication, 47% of non-experts ($N = 8$) preferred security keys. Nearly all of them preferred code delivery via text messages, all of them favored applications, and 14 preferred code delivery using emails. In contrast to experts, the majority ($N = 13$) of non-expert users did not express negative opinions about security questions; however, they were concerned ($N = 5$) about biometrics. A few non-expert users were also unfamiliar with security key technology.

Mandated Usage and High-Value Accounts: We assessed users' willingness to protect high-value assets using multi-factor authentication. Among average and expert users, most of them expressed an intention to protect critical accounts using some sort of MFA technology:

"So like social media I know for your emails likely they will. I just feel like it is a lot more useful than people take it for. I really, I honestly think that security wise which is one of the biggest things now and MFA is such a big thing that keeps your information safe" (P1, Expert)

"I would be more careful about my bank account, bank accounts should be secured." (P3, Non-expert)

Surprisingly, when we asked users about what they were currently using for multi-factor authentication, a significant portion of participants (experts and non-experts) said they only used the technology assigned by their organization. Some participants reported that they were unaware of other MFA technologies: *"Because I don't know of anymore...I only use Duo because that was the one provided to me"* (P1, Expert)

A few participants presented their understanding of multi-factor authentication using an illustration of the technology (Duo) that is widely deployed across organization as expressed in the sketch 6

Dependency on Mobile Devices: Both groups of users reported concerns about the dependency on mobile devices in current MFA implementations. This data is skewed by the fact that most of the users used a particular MFA app, Duo[1], which was suggested by their respective organization. A few participants mentioned security keys, but they noted that they do not know much about them. With Duo, there is a mobile device and

[1] https://duo.com/

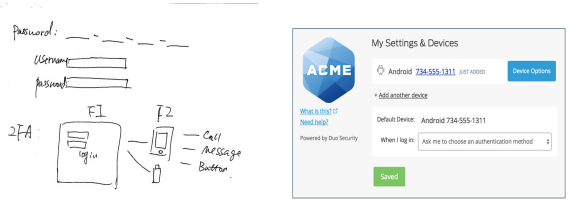

Figure 6. One Participant's Sketch (Left) that Demonstrated the Duo User Interface (Right).

application dependency; thus, the participants pointed out circumstances that caused temporary or permanent access interruption. While both groups expressed concerns about the dependency issue, experts insisted on having more security while not having a single point of failure. Non-experts provided problematic aspects of app-dependent MFA, such as connection issues or not having their phone accessible. None of them had knowledge of any fail-safe methods. *"Sometimes the Internet connection is not good with my phone"* (P2, Non-expert)

"My professor came to the lecture, then try to log in but he couldn't because he didn't have his phone. The lecture cancelled." (P2, Non-expert)

"My phone is died of battery, then I cannot reach my phone. The system is very time-consuming, it does not support disabilities especially I have a situation right now that on my hand, it burdens me with extra work in my busy life" (P3, Non-expert)

We analyzed these issues mentioned to enhance our implications in section 6:

- **Connection Issues**: User is unable to respond due to connection issues.
- **Battery Outage**: User is unable to respond to a multi-factor authentication challenge or view the TOTP code due to a power outage.
- **Device Presence**: User is unable to access the device in a short period of time.
- **Device Lost**: User is unable to access the device or even recover the account because it is lost.

5. Discussion

Our evaluation of risk perception levels revealed a primary reason for non-expert users failing to take security measurements seriously and enroll in multi-factor authentication. While a significant portion of users realized the catastrophic consequences and urgency of security threats, a few of them had trouble with understanding risk mitigation and protection. As a result, these users failed to utilize MFA. Table 2 summarizes participants and the expectations of multi-factor authentication use from these users. We found that most users believe that MFA is a good mechanism to enhance their information security. However, due to the knowledge differences between user groups, a few non-expert users believed that MFA is optional and not necessary at all times. Moreover, non-expert users would only apply MFA in workplace environments, which typically have IT management enforcement.

We see a positive correlation between expertise and MFA usage. Expert users have a good understanding of both computers and security, and they showed a respective understanding and utilization of multi-factor authentication. They understood operational knowledge and definitions of factors, as well as the risk of online applications and the coverage of protection. In contrast, non-experts occasionally failed to tell the difference between 2FA and MFA and treated it as a redundant security measure. As a result, our research identified a certain group of participants in information security that chose not to enroll in multi-factor authentication because they were confident in their existing security measures. These users had at least an average level of computer expertise. Users with poor computer expertise often lack security expertise, but the exit test results indicate that they have the potential for improvement. To ensure that multi-factor authentication is more accessible to average users, usability issues in current implementations need to be properly addressed.

The experts showed an active usage of multi-factor authentication, while other users had trouble with service discovery. In organization-wide scenarios, this issue was not revealed, since the information was clearly delivered to all users. For instance, in the sketches, a majority of users drew the Duo technology - which is utilized across the organization- instead of other common multi-factor authentication services. When it comes to a variety of online services, average users can have trouble locating security settings. The proactive way of prompting users to enable 2FA, however, might frustrate them during the login flow.

Regardless of user expertise, all users showed concerns regarding losing access to the companion device. Current threat models in multi-factor authentication do consider the case when a mobile device gets lost: sometimes a recovery code is provided, for instance. But there is no guarantee that users have properly stored it. In the survey, we found that average users are likely to experience circumstances such as data loss. In an organizational scenario, this vulnerability is mitigated by having a dedicated IT support person. However, it is necessary to introduce the recovery mechanism to average users in order to improve MFA adoption.

Addressing these issues uncovered by our findings would improve MFA usage within non-expert groups.

6. Implications

Our findings can be applied to improve MFA in a variety of ways. These include enhancing user education by putting more proactive information in the user interface, eliminating the sole dependency on mobile devices by introducing new verification technologies, and improving the procedures for disaster recovery.

User Interface Improvement: Non-experts occasionally encountered issues in service discovery. A feature that prompts for multi-factor authentication enrollment should be prompted immediately after their first successful password authentication. It might also be useful to move settings entries for multi-factor authentication to areas that are easier to discover (e.g. the home page of account settings).

Eliminate Mobile Dependency: Our findings

Category	Expert Users	Non-Expert Users
Risk Perception	Well understand and control	Less knowledge, have no mitigation and control
Mental Model of MFA	Additional factor and verification in authentication	Optional security service, lack of operational knowledge
MFA Usage Frequency	Frequent	Less-frequent
MFA Usage Scenarios	All accounts when possible	Specific, work-related

Table 2. Categories of Users and their Correlation with MFA

suggest that the dependency on mobile devices is one of the biggest roadblocks for the expansion of multi-factor authentication. Both groups of users expressed their distrust in the reliability of their mobile devices. To address the issue with mobile devices, new technologies can be developed to enable Secure Element [51] and remote attestation using trusted platform modules [52] for verifying the factor of "what you have." Additionally, environment fingerprinting and comparisons can be utilized for identifying a user's presence.

Proper and Effective Risk Communication: The evaluation of risk perception levels indicated that proper and effective risk communication from the service provider to the user is necessary in order to improve their awareness of information security. A possible solution is to use proactive notifications in services to allow the user to understand new security threats, as well as review security settings. To provide even better protection, service providers can suggest recommended security settings to users.

Factor Disaster Recovery: Our participants reported that the recovery procedures for account access in case of device loss are complicated and sometimes not possible. Current implementations [53] involve pre-generated passphrases for account recovery. Apart from eliminating the dependency on devices, such as phones, that are easy to lose or can be damaged beyond repair, a new mechanism that combines users' past activities and behavior into recovery can be developed as an overlapping authentication strategy. For instance, service providers could ask users ten questions about their behaviors in certain time periods for verifying their identity in the event of recovery.

Prioritized Authentication: Certain applications, such as online banking and stock exchange sites, need higher assurance levels during authentication. In other circumstances, users have preferences for authentication methods. A multi-factor authentication implementation could determine the importance of the authentication and select the proper authentication method based on the user's choice. This would give control to the user and thus enhance the user experience. However, it is worth noting that many users feel that their personal emails are not confidential or important enough, so proper risk communication is useful during such scenarios.

Time-Sensitive Adjustment: One usability issue users repeatedly mention is MFA occasionally causing interruptions when authenticating. For certain time-sensitive scenarios, current MFA implementations cannot satisfy users' needs. A new MFA implementation that recognizes and adjusts configuration settings based on a service application's priority can be implemented. This can be achieved through a trusted device implementation, where frequently used devices could be trusted during times when users have a meeting. Work devices often have their calendar linked, so this can be achieved.

Removal of Redundant Authentication: Current MFA technology often comes with duplicated factors. Despite the fact that the factor of possession (phone) has already been verified when a user logs in to a site via their phone's browser, MFA implementations send requests to the phone for confirmation. In such situations, MFA implementations can check for factors that verify the device's possession, such as the device identifier [54] or browser and sensor fingerprinting [55] to speed up the authentication process.

7. Limitations and Future Work

Our analysis of individuals' mental models regarding authentication technologies provides several opportunities for future research on the user experience and multi-factor authentication. In section 6, we propose potential solutions that involve changes in the user interface of online applications and technologies with MFA implementations. The effectiveness of these suggestions needs to be validated using empirical studies. Due to the qualitative nature of our study, our findings are derived from a small sample. To assess external validity, a large-scale online questionnaire could be developed based on these findings for a broader population. However, the qualitative nature of the study helped us get in-depth knowledge of users' risk perception, MFA usage, and frustration, which large-scale studies might fail to capture. Although we focused on general implementations of multi-factor authentication, further research is needed to examine the differences between specific technologies. While we collected important information to answer our specific RQs, we did not collect demographic data, such as gender and race, for privacy consideration; thus, future work can expand the research to learn about demographic and cultural differences.

8. Conclusion

Multi-factor authentication is an important defense against information security breaches in the modern connected world. It mitigates the risks of password breaches in the wake of increasingly frequent online attacks. While expert technology users have a good understanding of authentication and online security threats, a significant portion of Internet users are not experts in technology. These non-experts are less likely to take necessary actions for mitigating risks and protecting their online data security. Comprehensive

security can only be achieved by enhancing the usability of security tools. Our research on the mental models of MFA users emphasizes the importance of understanding their risk perceptions. From a technological perspective, improvements on MFA should be made to provide more accessible tools that cater to users without technical backgrounds. To improve users' risk awareness, proper and effective communication and education on risks and security measurements should be established by service providers and administrators. Promoting complete understanding of authentication concepts and security awareness is important for expanding the usage of multi-factor authentication and reducing the risks of future cyberattacks.

9. Acknowledgments

This research was supported in part by the National Science Foundation under CNS 1565375, Cisco Research Support, and the Comcast Innovation Fund. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the the US Government, the National Science Foundation, Cisco, Comcast, nor Indiana University. We would like to thank Ebuka Egbunam and HyeonJung Lee for helping with data collection, transcription, and analysis, and the Center for Applied Cybersecurity Research (CACR), who provided the platform to conduct the initial study.

References

[1] S. Das, A. Kim, Z. Tingle, and C. Nippert-Eng, "All about phishing: Exploring user research through a systematic literature review," *arXiv preprint arXiv:1908.05897*, 2019.

[2] B. Team, "Must-know phishing statistics 2018."

[3] R. Heiland, S. Koranda, S. Marru, M. Pierce, and V. Welch, "Authentication and authorization considerations for a multi-tenant service," in *Proceedings of the 1st Workshop on The Science of Cyberinfrastructure: Research, Experience, Applications and Models*, pp. 29–35, ACM, 2015.

[4] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021–2040, 2003.

[5] M.-S. Hwang and L.-H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on consumer Electronics*, vol. 46, no. 1, pp. 28–30, 2000.

[6] A. Oberle, P. Larbig, R. Marx, F. G. Weber, D. Scheuermann, D. Fages, and F. Thomas, "Preventing pass-the-hash and similar impersonation attacks in enterprise infrastructures," in *Advanced Information Networking and Applications (AINA), 2016 IEEE 30th International Conference on*, pp. 800–807, IEEE, 2016.

[7] R. Joyce, "Disrupting nation state hackers," *USENIX Enigma. San Fransisco, CA*, 2016.

[8] M. A. Ward, "Information systems technologies: A public-private sector comparison," *Journal of Computer Information Systems*, vol. 46, no. 3, pp. 50–56, 2006.

[9] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *2012 IEEE Symposium on Security and Privacy*, pp. 553–567, IEEE, 2012.

[10] S. Das, A. Kim, B. Jelen, J. Streiff, L. J. Camp, and L. Huber, "Towards implementing inclusive authentication technologies for older adults," *Who Are You*, 2019.

[11] A. Amin, I. ul Haq, and M. Nazir, "Two factor authentication," *International Journal of Computer Science and Mobile Computing*, 2017.

[12] D. M. Ting, O. Hussain, and G. LaRoche, "Systems and methods for multi-factor authentication," Aug. 25 2015. US Patent 9,118,656.

[13] J.-J. Kim and S.-P. Hong, "A method of risk assessment for multi-factor authentication," *Journal of Information Processing Systems*, vol. 7, no. 1, pp. 187–198, 2011.

[14] X. Huang, Y. Xiang, E. Bertino, J. Zhou, and L. Xu, "Robust multi-factor authentication for fragile communications," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 6, pp. 568–581, 2014.

[15] S. Das, G. Russo, A. C. Dingman, J. Dev, O. Kenny, and L. J. Camp, "A qualitative study on usability and acceptability of yubico security key," in *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*, pp. 28–39, ACM, 2018.

[16] E. R. Potter, "Multi-factor authentication using a one time password," Oct. 9 2008. US Patent App. 11/697,881.

[17] C. Adams and M. J. Wiener, "Multi-factor biometric authenticating device and method," Mar. 26 2002. US Patent 6,363,485.

[18] A. P. Sabzevar and A. Stavrou, "Universal multi-factor authentication using graphical passwords," in *Signal Image Technology and Internet Based Systems, 2008. SITIS'08. IEEE International Conference on*, pp. 625–632, IEEE, 2008.

[19] M. M. Althobaiti and P. Mayhew, "Security and usability of authenticating process of online banking: User experience study," in *Security Technology (ICCST), 2014 International Carnahan Conference on*, pp. 1–6, IEEE, 2014.

[20] J. Lang, A. Czeskis, D. Balfanz, M. Schilder, and S. Srinivas, "Security keys: Practical cryptographic second factors for the modern web," in *International Conference on Financial Cryptography and Data Security*, pp. 422–440, Springer, 2016.

[21] S. Das, A. Dingman, and L. J. Camp, "Why johnny doesn't use two factor a two-phase usability study of the fido u2f security key," in *2018 International Conference on Financial Cryptography and Data Security (FC)*, 2018.

[22] S. Das, B. Wang, Z. Tingle, and J. Camp, "Evaluating user perception of multi-factor authentication: A systematic review." unpublished.

[23] S. Das, B. Wang, and L. J. Camp, "Mfa is a waste of time! understanding negative connotation towards mfa applications via user generated content," in *Proceedings of the Thriteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019)*, 2019.

[24] C. Braz and J.-M. Robert, "Security and usability: The case of the user authentication methods," in *IHM*, vol. 6, pp. 199–203, 2006.

[25] D. McCoy, K. Bauer, D. Grunwald, P. Tabriz, and D. Sicker, "Shining light in dark places: A study of anonymous network usage," *University of Colorado Technical Report CU-CS-1032-07 (August 2007)*, 2007.

[26] A. Whitten and J. D. Tygar, "Why johnny can't encrypt: A usability evaluation of pgp 5.0.," in *USENIX Security Symposium*, vol. 348, 1999.

[27] J. Armington and P. Ho, "Robust multi-factor authentication for secure application environments," Aug. 28 2003. US Patent App. 10/086,123.

[28] U. Maurer, "Modelling a public-key infrastructure," in *European Symposium on Research in Computer Security*, pp. 325–350, Springer, 1996.

[29] H. Hadan, N. Serrano, S. Das, and L. J. Camp, "Making iot worthy of human trust," *Available at SSRN 3426871*, 2019.

[30] C. J. Hessler, "Method for mobile security via multi-factor context authentication," Jan. 13 2015. US Patent 8,935,769.

[31] A. K. Nag and D. Dasgupta, "An adaptive approach for continuous multi-factor authentication in an identity eco-system," in *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, CISR '14, (New York, NY, USA), pp. 65–68, ACM, 2014.

[32] X. Huang, Y. Xiang, E. Bertino, J. Zhou, and L. Xu, "Robust multi-factor authentication for fragile communications," p. 1, 2014.

[33] M. A. Kampe and A. Hisgen, "System and method for comprehensive availability management in a high-availability computer system," Feb. 10 2004. US Patent 6,691,244.

[34] A. Bhargav-Spantzel, A. C. Squicciarini, S. Modi, M. Young, E. Bertino, and S. J. Elliott, "Privacy preserving multi-factor authentication with biometrics," *Journal of Computer Security*, vol. 15, no. 5, pp. 529–560, 2007.

[35] Q. Jiang, Z. Chen, B. Li, J. Shen, L. Yang, and J. Ma, "Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 4, pp. 1061–1073, 2018.

[36] A. Paepcke, "Information needs in technical work settings and their implications for the design of computer tools," *Computer Supported Cooperative Work (CSCW)*, vol. 5, no. 1, pp. 63–92, 1996.

[37] P. Rajivan, P. Moriano, T. Kelley, and L. J. Camp, "Factors in an end user security expertise instrument," *Information Computer Security*, vol. 25, no. 2, pp. 190–205, 2017.

[38] K. Gallagher, S. Patil, and N. Memon, "New me: Understanding expert and non-expert perceptions and usage of the tor anonymity network," in *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pp. 385–398, USENIX Association, 2017.

[39] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," *Computers Security*, vol. 24, no. 2, pp. 124 – 133, 2005.

[40] Y. Albayram, M. M. H. Khan, and M. Fagan, "A study on designing video tutorials for promoting security features: A case study in the context of two-factor authentication (2fa)," *International Journal of Human–Computer Interaction*, vol. 33, no. 11, pp. 927–942, 2017.

[41] C. S. Weir, G. Douglas, T. Richardson, and M. Jack, "Usable security: User preferences for authentication methods in ebanking and the effects of experience," *Interacting with Computers*, vol. 22, no. 3, pp. 153–164, 2010.

[42] J. Reynolds, T. Smith, K. Reese, L. Dickinson, S. Ruoti, and K. Seamons, "A tale of two studies: The best and worst of yubikey usability," in *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 872–888, IEEE, 2018.

[43] J. Colnago, S. Devlin, M. Oates, C. Swoopes, L. Bauer, L. Cranor, and N. Christin, "it's not actually that horrible: Exploring adoption of two-factor authentication at a university," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, p. 456, ACM, 2018.

[44] L. J. Camp, "Mental models of privacy and security," *IEEE Technology and society magazine*, vol. 28, no. 3, pp. 37–46, 2009.

[45] F. Asgharpour, D. Liu, and L. J. Camp, "Mental models of security risks," in *International Conference on Financial Cryptography and Data Security*, pp. 367–377, Springer, 2007.

[46] A. R. Kearney and S. Kaplan, "Toward a methodology for the measurement of knowledge structures of ordinary people: The conceptual content cognitive map (3cm)," *Environment and Behavior*, vol. 29, no. 5, pp. 579–617, 1997.

[47] V. Garg and J. Camp, "End user perception of online risk under uncertainty," in *2012 45th Hawaii International Conference on System Sciences*, pp. 3278–3287, IEEE, 2012.

[48] B. B. Kawulich, "Data analysis techniques in qualitative research," *Journal of Research in Education*, vol. 14, no. 1, pp. 96–113, 2004.

[49] L. J. Camp, "Mental models of computer security," in *International Conference on Financial Cryptography*, pp. 106–111, Springer, 2004.

[50] D. Liu, F. Asgharpour, and L. J. Camp, "Risk communication in security using mental models," *Usable Security*, vol. 7, 2008.

[51] A. Hammad, "Integration of payment capability into secure elements of computers," Aug. 23 2016. US Patent 9,424,413.

[52] D. Schellekens, B. Wyseur, and B. Preneel, "Remote attestation on legacy operating systems with trusted platform modules," *Science of Computer Programming*, vol. 74, no. 1-2, pp. 13–22, 2008.

[53] D. Hardt, "Multi-factor authentication with recovery mechanisms," Dec. 16 2010. US Patent App. 12/866,466.

[54] A. Chowdhury, G. Breznik, K. Verdnik, and B. Prihavec, "Customer identification and authentication procedure for online internet payments using mobile phone," Jan. 17 2012. US Patent 8,099,077.

[55] H. Bojinov, Y. Michalevsky, G. Nakibly, and D. Boneh, "Mobile device identification via sensor fingerprinting," *arXiv preprint arXiv:1408.1416*, 2014.